UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Dropbox ID User # 3087809008, username of "Brandon Gilmore" and email address of thememuzickent@gmail.com	)	Case No.22-985M(NJ) **Matter No.: 2022R00300**

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 9, 2022 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued:8/26/2022 @ 3:20 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is the entire digital contents of the Dropbox account(s) associated with the following Dropbox subscriber name:

Dropbox ID User # 3087809008, username of "Brandon Gilmore" and email address of thememuzickent@gmail.com and all its associated services including deleted files and e-mails; IP addresses and associated dates/times used to access the e-mail account; activity history; that is/are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107.

ATTACHMENT B

Particular Items to be Seized

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A.

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including activity history, log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account(s) associated with the Dropbox link files referenced in Attachment A pertaining to the possession and distribution of child pornography images and/or videos.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to Special Agent Daniel Gartland at: Federal Bureau of Investigation, 3600 South Lake Drive, St. Francis, Wisconsin 53235.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Dropbox ID User # 3087809008, username of "Brandon Gilmore" and email address of thememuzickent@gmail.com

Case No. 22-985M(NJ)

Matter No.: 2022R00300

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2256(8); § 2256 (2);	Possession, receipt or distribution of child pornography; possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct.

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Daniel Gartland, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 8/26/2022

Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., an online, electronic file storage provider headquartered at 185 Berry Street, 4th Floor, San Francisco, California 94107. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May of 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force.

3. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have also received training and

gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

4. This affidavit is based upon my personal knowledge, my training and experience, and on information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, official records, citizen witnesses' statements, consent searches, recorded statements, law enforcement surveillance, surveillance video, social media, court records, telephone records, and public records which I consider to be reliable as set forth herein. The facts of this Affidavit are based upon information obtained from my investigation, as well as information I have received from other law enforcement officers.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography, have been committed by Brandon Gilmore (XX/XX/1989). There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

DEFINITIONS

6. The following definitions apply to the Affidavit and Attachments A and B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones

or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer Server" or "Server," is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in

essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A

password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data,

called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. "An Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC

address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

PROBABLE CAUSE

6. On May 9, 2022, the National Center for Missing and Endangered Children (NCMEC) received information from Dropbox, Inc. (Dropbox) that suspected Child Sexual Abuse Material (CSAM) was uploaded to the Dropbox account belonging to user Brandon Gilmore. The following user information was provided:

a. Email address: thememuzickent@gmail.com

b. Screen/username: Brandon Gilmore

7. Dropbox provided six videos uploaded to the account associated with user Brandon Gilmore. NCMEC provided the information to the Federal Bureau of Investigation for further action. The first video showed a female removing her clothes and touching her vagina. The video then showed an adult male touch her vagina and engaged in vaginal and anal sex with the female. The female appeared to be in the early stages of puberty with minor breast development and some pubic hair. The second video showed adult male engaged in vaginal sex with a minor female. The female appeared to be pre-pubescent, lacking pubic hair and breast development. The third video showed an adult male engaged in oral sex with a minor female. The female wore a blindfold over her eyes. The words, "suck cock cum slut" were written on the blindfold. The female had facial features consistent with a pre-pubescent child. The fourth video showed a close-up view of an adult male engaged in vaginal sex with a pre-pubescent female, lacking pubic hair. The fifth video depicted an adult male laying on a bed while two unclothed females removed his pants and touched his penis and testicles. The females appeared to be pre-pubescent, lacking breast development and pubic hair. The sixth video showed a female sitting on a chair with her pants pulled down. An adult male then lifted her legs displaying her anus and vagina. The video then showed the male spreading open the minor female's vagina. The female appeared to be pre-pubescent, lacking breast

development and pubic hair. The female also wore a t-shirt with a cartoon drawing of a smiling sun. An upload log provided by Dropbox indicated the videos were uploaded on or about May 7, 2022.

8. On June 6, 2022, Dropbox provided information in response to a subpoena requesting user account information and IP addresses associated with the Dropbox user Brandon Gilmore. The information revealed that the account was accessed by IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e on May 7, 2022.

9. Further investigation determined that the IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e was assigned to an AT&T account with the following subscriber information:

i. Account Number: 314010876

ii. Subscriber Name: Brianna Roeck

iii. Account Creation: 06/11/2021

iv. Service Address: 3640 South 87th Street, Milwaukee, WI, 53228

10. A search of law enforcement databases revealed that in June of 2021 Brandon Gilmore (XX/XX/1989) was involved in a vehicular accident in Milwaukee, WI, while driving a black Chevrolet Equinox bearing Wisconsin registration plate ACS-3373 (hereinafter "Equinox"). The registered owner of the Equinox was Brianna Roeck. Gilmore also owns a blue 2004 Chevrolet Impala registered with the state of Wisconsin at the address 3640 South 87th Street, Milwaukee, WI.

11. On July 25, 2022, Special Agents with the Federal Bureau of Investigation (FBI) observed Brianna Roeck arrive at 3640 South 87th Street, Milwaukee, WI, driving the Equinox.

Agents observed Gilmore leave the address and return while driving the Equinox. Agents also observed a blue Impala without visible plate parked at the address.

12. An open-source search of Facebook revealed a profile with the name, "Brianna Röck." The profile includes references to the "Gilmore's" and includes photos that appear to show Brianna Roeck and Brandon Gilmore together. The profile also contains references to Brynlee Gilmore, a baby born in early-October 2021 and photos of two other female children. Based upon the information in the Facebook profile, I believe Brianna Roeck and Brandon Gilmore are in a relationship.

13. A search of law enforcement databases revealed that Brandon Gilmore is a registered sex offender and resides at the address 3640 South 87th Street, Milwaukee, WI. On July 23, 2013, Gilmore was arrested by the FBI in Minneapolis, MN for a violation of Title 18 U.S.C. § 2423 (d) and (e) Conspiracy to Facilitate in Transportation of Minors for Prostitution. The arrest was the result of an investigation into Gilmore and two other females for the transportation of a 14-year-old female from Milwaukee, WI to Bloomington, MN for the purpose of engaging in prostitution. Gilmore plead guilty to the charge and was sentenced to 82 months in federal prison and 60 months of supervised release. Gilmore remained on supervision with the United States Probation Office for the Eastern District of Wisconsin as of July 26, 2022 and was due to complete his supervision on August 13, 2024.

14. On July 27, 2022, a search warrant, issued in the United States District Court for the Eastern District of Wisconsin on July 27, 2022, was executed by the FBI at 3640 South 87th Street, Milwaukee, WI. During the search, law enforcement officers seized as evidence an Apple iPhone 13 with serial number: DPQ00N306, (hereinafter, "the Phone") from the location. Pursuant to the search warrant, a forensic examination of the phone. The was assigned telephone number

414-708-5314 and had an Apple ID associated with the e-mail address, thememuzickent@gmail.com.

15. The Phone appeared to have an initial power on date of June 26, 2022. The phone included data from dates prior to the initial power on date. Based on my training and experience, I believe the user of the phone obtained a new device on or about June 26, 2022 and synced the Phone with data maintained in on an external cloud-based server.

16. The phone contained several social media accounts and associated conversations. A Facebook profile and Facebook Messenger account on the phone was associated with the username Charles Palmer with the identification number 10006618555099. A Kik messenger account with a username of "bgillie08" and the e-mail address, Ovathatop01@gmail.com. The Apple wallet for the Phone was associated with "Brandon Gilmore" at the address 4597 North Houston Avenue, Milwaukee, WI. Law enforcement databases indicate that 4597 North Houston Avenue, Milwaukee, WI is the address of Tequila Matthews, mother of Brandon Gilmore.

17. Investigators conducted a review of Kik messenger conversations recovered from the telephone. At least two conversations contained discussions of Child Sexual Abuse Material (CSAM). On July 17, 2022, Kik user "claraoglyta_cb5" (hereinafter, "CB5") initiated a conversation with the account associated with the phone. CB5 asked "Are you a buyer of cp mega link and video?" CB5 further provided an apparent list of the types of CSAM available. Bgillie08 responded "Samples." A link to at least one video of suspect CSAM was sent to Bgillie08 and a request for payment was made. On July 25, 2022, Bgillie08 messaged "Samples" to Claraoglyta_cb5, though the message did not appear to be delivered.

18. A Kik conversation between bgillie08 and dirtydaughter101_n1k (hereinafter, "N1K") occurred from July 17, 2022 to July 25, 2022. The conversation began with N1K sending

links of known or suspected CSAM to Bgillie08 and a request to "Send me the screenshot baby." Bgillie08 responds with a screenshot of a $50 payment via an electronic funds transfer application to a user named "Malacia Hyche." Bgillie08 then messages, "Penetration and cum" and "And anal." N1K then provided additional videos. Bgillie08 later states, "I'll send more money when I have all 50 videos u promised for the 30 I sent." After receiving a series of videos, Bgillie08 states, "That's not cp. That don't count." Further videos and requests for money were sent from N1K until July 19, 2022. On July 25, 2022, the conversation ended with Bgillie08 asking, "Samples?"

19. Investigators conducted a review of the images and videos recovered from the Phone. The phone contained numerous selfie-style images of Brandon Gilmore, including metadata with a location in the area of 3640 South 87th Street, Milwaukee, WI. The phone contained approximately 34 videos of known or suspected CSAM. Five of these videos are further described as follows:

- A close-up video of an infant, approximately less than one year of age, with a white fabric background. The child did not appear to have developed lower teeth. The child's bare chest was visible in the video. The child appeared to be Caucasian, though hair color and sex of the child could not be determined based upon the view of the camera. An erect adult penis was inserted into the child's mouth during the video. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately four to eight years of age, laying on her back with her legs held up. The female had short dark brown or black hair and a light skin tone. The child did not have developed breasts or pubic hair. The child's mannerisms were consistent with a mental handicap. Written on the inner thigh of the child's left leg is the letter "I", a drawing of a heart and an illegible word. The female child was completely

naked, and her anus and vagina were clearly visible. There was apparent male ejaculate on the child's legs, vagina and seeping from her anus. A white-skinned adult hand with manicured fingernails pointed to the ejaculate in the child's anus. The video appeared to have been recovered from applications on the Phone.

- A video of a pre-pubescent female, approximately five to nine years of age, visible from the mid-torso down. The child was light skinned. Her face and hair were not visible in the video. The female was wearing a pink and white striped bathing suit with a pink and blue flowers or starfish pattern. The child's bathing suit was pushed to the side and her vagina was partially visible. A white skinned adult male penis had vaginal sex with the child. The adult male's right hand was pressed down on the child's stomach area. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately five to nine years of age, standing in front of a white skinned adult male. The female child is light skinned with short brown hair. The female was wearing a white T-shirt and did not appear to be clothed from the waist down. The female did not appear to have developed breasts. The adult male was wearing a white T-shirt pulled up above his belly button. The adult male has the child perform oral sex on him. The adult male had one hand on the child's shoulder and the other hand manipulated the zoom on a camera with a remote. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately two to six years of age, lying on a carpeted floor. The child was light skinned. The child did not have pubic hair. Her face and hair were not visible in the video. The child appeared to be wearing a green T-shirt, pulled up above her chest. The child's vagina was clearly visible in the video. A dark-skinned

adult male with an erect penis had anal and vaginal sex with the child before ejaculating on the child's pubic area. The adult male held the child down at various points in the video by gripping the child's waist. The video appeared to have been recovered from applications on the Phone.

20. On July 27, 2022, Brandon Gilmore was interviewed by Special Agents of the FBI in a non-custodial setting at the FBI Milwaukee Field Office. During the interview, Gilmore stated that he had a Dropbox account when he was first released from prison. The account was registered with the e-mail address thememuzickent@gmail.com. Gilmore maintained a few self-developed rap songs on the account and had not used it in several years. Gilmore also used the e-mail address ovathatop01@gmail.com. Gilmore provided the pass code to his phone and stated that he did not have Dropbox on the phone. He further stated that there was not child pornography on his phone. Gilmore stated he "was not concerned about child pornography" and "did not watch child pornography."

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

21. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc.to disclose to the government copies of the records and other information, including the content of communications, particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

22. Based on the forgoing, I request that the Court issue the proposed search warrant because there is probable cause to believe that evidence of a criminal offense, namely, a violation

of 18 U.S.C. § 2252A, is located within Dropbox account(s) associated with Dropbox link files, which are more fully described in Attachment A, which is incorporated herein by reference.

23. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

The property to be searched is the entire digital contents of the Dropbox account(s) associated with the following Dropbox subscriber name:

Dropbox ID User # 3087809008, username of "Brandon Gilmore" and email address of thememuzickent@gmail.com and all its associated services including deleted files and e-mails; IP addresses and associated dates/times used to access the e-mail account; activity history; that is/are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107.

ATTACHMENT B

Particular Items to be Seized

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A.

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including activity history, log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account(s) associated with the Dropbox link files referenced in Attachment A pertaining to the possession and distribution of child pornography images and/or videos.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to Special Agent Daniel Gartland at: Federal Bureau of Investigation, 3600 South Lake Drive, St. Francis, Wisconsin 53235.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Dropbox, Inc. and my official title is _____. I am a custodian of records for Dropbox, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Dropbox, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Dropbox, Inc.; and

c. such records were made by Dropbox, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date	Signature